Problemen oplossen met LISP VXLAN Fabric op Catalyst 9000-serie Switches

Inhoud

Inleiding

In dit document worden de basiscomponenten van een op LISP VXLAN gebaseerde verbinding beschreven en wordt beschreven hoe de werking ervan kan worden gecontroleerd.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Cisco IOS XE 17.9.3 of hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

LISP VXLAN-gebaseerde verbinding

Het doel van het implementeren van een LISP VXLAN-netwerk is om een architectuur te kunnen maken waarbij meerdere Overlay-netwerken, ook wel Virtual Networks genoemd, bovenop een onderliggend netwerk worden gedefinieerd.

- Het Underlay-netwerk in een dergelijke topologie zou voornamelijk fungeren als een transportlaag en zou zich niet bewust zijn van de overlay-topologieën die eroverheen worden gerund.
- Overlay-netwerken kunnen worden toegevoegd en verwijderd zonder invloed op het onderliggende netwerk.
- Het gebruik van overlaynetwerken scheidt de gebruikers effectief van het onderliggende netwerk.

Technologieën die worden gebruikt om een LISP VXLAN-verbinding te maken

Locator Identity Separation Protocol (LISP)

- Het LISP-protocol is het controlevliegtuigprotocol dat in de fabric wordt gebruikt. Het werkt op alle fabric-apparaten om de fabric te bouwen en te bepalen hoe het verkeer door de fabric wordt verzonden.
- LISP maakt 2 adresruimten. Een daarvan is voor de Routing Locator (RLOC's) die worden gebruikt om bereikbaarheid te adverteren. De andere adresruimte is voor de Endpoint Identifiers (EID) , waar de eindpunten zich bevinden en wordt gebruikt voor de overlapping.

- Binnen LISP worden de EID's geadverteerd met een geadverteerd RLOC. Als een EID beweegt, hoeft u alleen de bijbehorende Routing Locator bij te werken.
- Om een eindpunt met LISP-verkeer naar een EID te bereiken, moet het worden ingekapseld en getunneld naar het RLOC dat het ontkapselt en doorstuurt naar het eindpunt.

Groepsgebaseerd beleid

- Er wordt gebruikgemaakt van segmentatie binnen een op een stoffengroep gebaseerd beleid.
- Wanneer op groepen gebaseerd beleid wordt geïmplementeerd, wordt het verkeer geclassificeerd met Secure Group in plaats van op basis van het IP-adres van de bron/bestemming.
- Dit vermindert de complexiteit van complexe toegangscontrolelijsten. In plaats van lijsten met IP-adressen die moeten worden onderhouden, worden IP-adressen / subnetten toegewezen aan een Secure Group Tag.
- Bij het binnendringen in de stof wordt gelabeld met een SGT wanneer het verkeer de stof verlaat, wordt de bestemming van het frame opgezocht voor zijn SGT.
- Met het gebruik van een matrix worden de bron en de bestemming SGT gematcht en wordt een Secure Group ACL toegepast om het verkeer af te dwingen wanneer het de fabric verlaat.

VXLAN-inkapseling

- Binnen de fabric wordt VXLAN gebruikt om al het verkeer in te kapselen
- Het voordeel van het gebruik van VXLAN ten opzichte van de bestaande LISP-inkapseling is dat het mogelijk is om het volledige Layer 2-frame in te kapselen, niet alleen het Layer 3-frame. Omdat het hele frame wordt ingekapseld, kunnen overlays zowel laag 2 als laag 3 zijn.
- VXLAN maakt gebruik van UDP met bestemmingspoort 4789. Hierdoor kunnen LISP VXLAN-frames ook worden getransporteerd via apparaten die zich niet bewust zijn van de overlay-topologie.
- Aangezien VXLAN het hele frame omvat, is het belangrijk om de MTU te verhogen, zodat er geen fragmentatie nodig is omdat er verkeer wordt verzonden tussen RLOC's. Alle tussenliggende apparaten zouden een grotere MTU moeten ondersteunen om de ingekapselde frames te vervoeren.

Verificatie

- Om eindpunten aan hun respectievelijke bronnen toe te kunnen wijzen, kan authenticatie worden gebruikt.
- Met protocollen als 802.1x kunnen MAB- en Webauth-eindpunten worden geverifieerd en / of geprofileerd tegen een Radius-server en toegang krijgen tot het netwerk op basis van hun autorisatieprofielen.
- Met hun respectieve Radius-attributen kunnen eindpunten worden toegewezen aan hun respectieve VLAN, SGT en andere attributen om een toegangspunt voor het eindpunt/gebruikersnetwerk te bieden.

Belangrijkste onderdelen in LISP VXLAN Fabric

knooppunt regelvlak

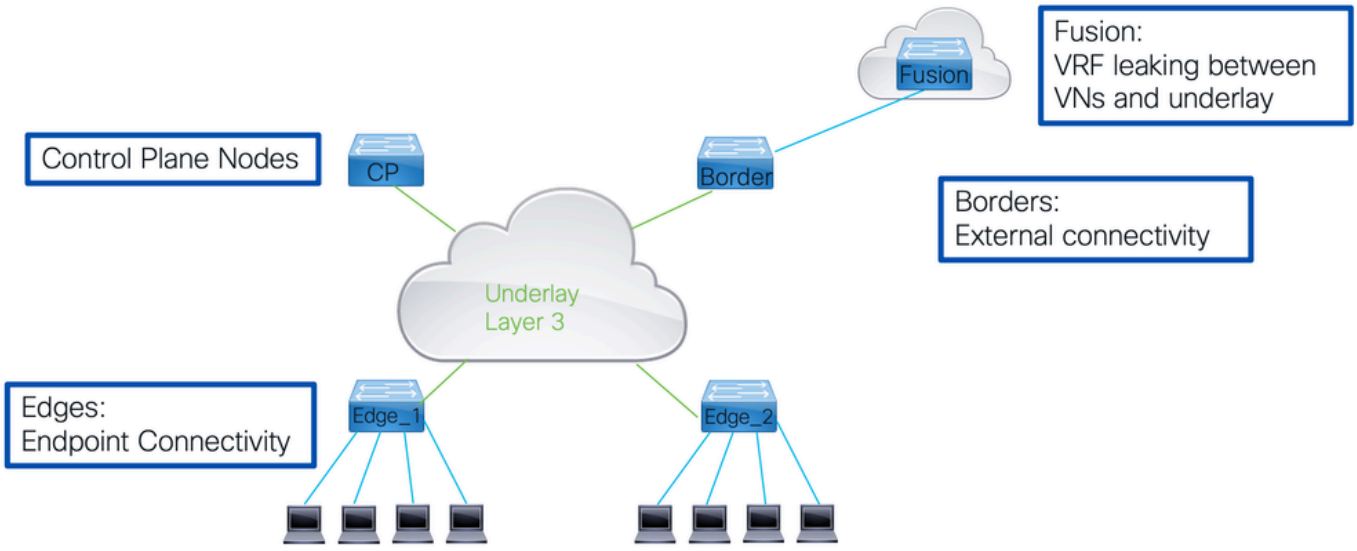
- bevat de LISP Map Server- en Map Resolver-functionaliteit.
- Alle andere weefselapparaten vragen de knooppunt van het regelvlak om de locatie van EID en sturen registraties voor hun EID naar de knooppunten van het regelvlak.
- Dit geeft de Control Plane knooppunten een compleet beeld van de stof met betrekking tot wat RLOC de verschillende EID zijn.

Randknooppunten

- Biedt connectiviteit buiten de stof met andere stoffen of met de buitenwereld.
- Interne grenzen importeren routes in de structuur en registreren deze met de knooppunten van het controlevlak.
- Externe grenzen maken verbinding met de buitenwereld en bieden een standaardpad buiten de structuur voor onbekende IP-bestemmingen.

Randknooppunten

- Deze knooppunten bieden connectiviteit met eindpunten in de fabric.
- In de definitie van LISP zouden dit XTR's zijn, omdat ze zowel de functie van een Ingress Tunnel Router (ITR) als een Egress Tunnel Router (ETR) zouden uitvoeren.



Nodes zijn niet beperkt tot het uitvoeren van slechts één taak.

- Ze kunnen een combinatie of zelfs alle functies in de stof uitvoeren.
- Wanneer een knooppunt van een grensknooppunt en een controlevlak zich op één apparaat bevinden, worden ze gecolocatie genoemd.
- Als dat knooppunt ook de Edge-functionaliteit biedt, wordt het een Fabric In A Box (FIAB)

genoemd.

Grenzen bieden overdrachten aan de rest van het netwerk om VRF lite te gebruiken.

- Elke overlay of een virtueel netwerk is gekoppeld aan een VRF-instantie op de border node.
- Om die verschillende VRF's aan elkaar te koppelen wordt een Fusion router gebruikt. Die fusion-router maakt geen deel uit van de Fabric zelf, maar is cruciaal voor de werking om de Overlay-netwerken op de fabric te kunnen aansluiten.

Een ander belangrijk concept binnen een LISP VXLAN-fabric is het concept om een IP-anycast te gebruiken.

- Dit betekent dat op alle Edge-apparaten het IP-adres en de MAC-adressen voor de geschakelde virtuele interfaces (SVI) worden gerepliceerd.
- Elke Edge heeft dezelfde configuratie op de SVI met betrekking tot IPv4-, IPv6- en MAC-adressen.
- Om dit probleem op te lossen, zijn er enkele uitdagingen.
    - Om de bereikbaarheid te testen met ping werkt met lokale aangesloten apparaten.
    - Als u externe bestemmingen wilt bereiken via de LISP VXLAN-structuur, wordt geen antwoord geretourneerd omdat het apparaat dat een antwoord verzendt dit ook verzendt naar het anycast IP-adres dat wordt gepunteerd op het lokale fabric-apparaat dat niet weet welke andere fabric-node de oorspronkelijke ping heeft verzonden.

Eindpuntregistratie

Om een LISP VXLAN-fabric te laten werken, is het van cruciaal belang dat de knooppunt Control Plane weet hoe alle eindpunten via de fabric kunnen worden bereikt.

- Voor het controlevlak om meer te weten te komen over alle EID's in het netwerk, is het afhankelijk van alle andere weefselapparaten om alle EID's te registreren die het kent met het controlevlak.
- Een fabric node verzendt LISP map-register berichten naar de control plane node. Onder de informatie die wordt geadverteerd met de kaart-register bericht.

Belangrijke informatie

LISP-instantie-id:

- Deze id wordt door de fabric gedragen en geeft aan welk virtueel netwerk moet worden gebruikt.
- Binnen een LISP VXLAN-fabric per Layer 3-overlay wordt één instantie per gebruikt VLAN in de fabric gebruikt, maar er is ook een Layer 2-instantie.

Eindpunt geïdentificeerd (EID):

- Als dit een Layer 2- of Layer 3-instantie is, is dit het MAC-adres, de IP-hostroute (/32 of /128) of een geregistreerd IP-subnet

Routing Locator (RLOC):

- Dit is het fabric-knooppunt met een eigen IP-adres waarmee het bereikbaarheid adverteert waar andere fabric-apparaten ingekapseld verkeer verzenden dat het EID zou moeten bereiken.

Proxyvlag:

- Wanneer deze vlag is ingesteld, kan de Control Plane-node direct reageren op toewijzingsverzoeken van andere fabric-nodes, zonder dat de proxy-vlag alle verzoeken heeft ingesteld om te worden doorgestuurd naar de fabric-node die de EID heeft geregistreerd.

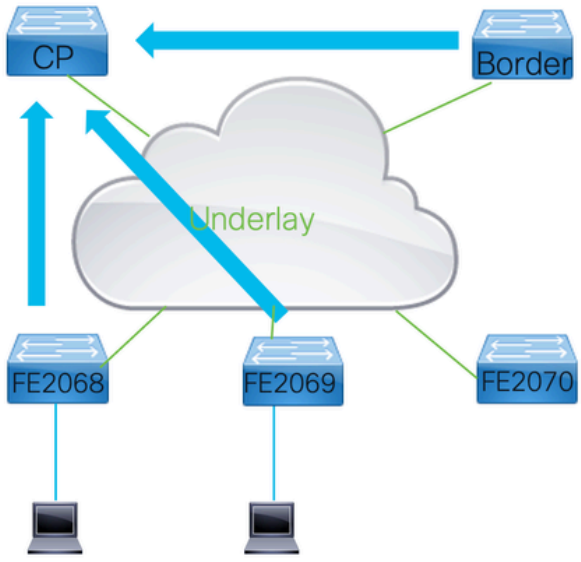
Registratiestappen

Stap 1: Fabric-apparaten leren over eindpuntidentificatoren. Dit kan zijn door middel van configuratie, routeringsprotocollen of wanneer het geleerd op de fabric-apparaten.

Stap 2: Fabric Devices registreren de geleerde eindpunten met elk bekend en bereikbaar Control Plane-knooppunt in de fabric.

Stap 3: Control Plane-knooppunten onderhouden een tabel met geregistreerde EID's met de bijbehorende Instance ID, de RLOC en de EID geleerd

Instance	RLOC	EID (mac address)
8189	FE2068	0019.3052.6d7f
8189	FE2069	0019.3052.6d7f
4099	FE2068	172.24.1.4/32
4099	FE2069	172.24.1.3/32
4099	Border	10.48.13.0/24



Verifiëren

1.1 MAC-adresinformatie

Voor Layer 2-instanties zijn de gebruikte EID de MAC-adressen die in het gekoppelde VLAN worden geleerd. Fabric Edges leren de Layer 2-adressen via standaardmethoden op de switches.

Zoek het VLAN dat is gekoppeld aan een specifieke Layer 2-instantie-id. De configuratie kan

worden beoordeeld of de opdracht

Gebruik "show lisp instance-id <instance> ethernet"

<#root>

```
FE2068#
show lisp instance-id 8191 ethernet

  Instance ID:
8191

  Router-lisp ID:                         0
  Locator table:                          default
  EID table:
Vlan 150

  Ingress Tunnel Router (ITR):            enabled
  Egress Tunnel Router (ETR):             enabled
  ..
  Site Registration Limit:                0
  Map-Request source:                     derived from EID destination
  ITR Map-Resolver(s):                    172.30.250.19
  ETR Map-Server(s):                      172.30.250.19
```

Zoals te zien is in de uitvoer, is de instance-id 8191 gekoppeld aan VLAN 150. Dat betekent dat alle MAC-adressen in het vlan worden geregistreerd bij LISP en onderdeel worden van de LISP VXLAN-structuur.

<#root>

```
FE2068#
show mac address-table vlan 150

          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 150    0000.0c9f.f18e    STATIC      Vl150

 150    0050.5693.8930    DYNAMIC     Gi1/0/1

 150    2416.9db4.33fd    STATIC      Vl150
```

```
 150    0019.3052.6d7f    CP_LEARN    L2LI0


Total Mac Addresses for this criterion: 3
Total Mac Addresses installed by LISP: REMOTE: 1
```

Statische vermeldingen met interface Vl150 zijn de MAC-adressen van de Switch Virtual Interface (interface vlan 150).

- Die MAC-adressen zijn niet geregistreerd bij de control plane node omdat ze hetzelfde zouden zijn op alle edge-apparaten.
- De weergegeven CP_LEARN-items zijn items die via de structuur zijn geleerd. Voor alle andere vermeldingen moeten ze, als ze dynamisch of statisch zijn, worden geregistreerd bij het knooppunt van het controlevlak.

Zodra ze via hun respectieve middelen zijn geleerd, verschijnen ze in de lisp-database-uitgangen, deze uitvoer bevat alle lokale vermeldingen op dit weefselapparaat.

<#root>

```
FE2068#

show lisp instance-id 8191 ethernet database


LISP ETR MAC Mapping Database for LISP 0 EID-table

Vlan 150 (IID 8191)

, LSBs: 0x1
Entries total 3, no-route 0, inactive 0, do-not-register 2

0000.0c9f.f18e/48

, dynamic-eid Auto-L2-group-8191,

do not register

, inherited from default locator-set rloc_hosts
  Uptime: 14:56:40, Last-change: 14:56:40
  Domain-ID: local
  Service-Insertion: N/A
  Locator        Pri/Wgt  Source     State


172.30.250.44

  10/10   cfg-intf   site-self, reachable

0050.5693.8930/48

, dynamic-eid Auto-L2-group-8191, inherited from default locator-set rloc_hosts
  Uptime: 14:03:06, Last-change: 14:03:06
  Domain-ID: local
  Service-Insertion: N/A
  Locator        Pri/Wgt  Source     State


172.30.250.44
```

```
  10/10   cfg-intf   site-self, reachable
2

416.9db4.33fd/48

, dynamic-eid Auto-L2-group-8191, do not register, inherited from default locator-set rloc_hosts
  Uptime: 14:56:50, Last-change: 14:56:50
  Domain-ID: local
  Service-Insertion: N/A
  Locator        Pri/Wgt  Source     State


172.30.250.44

   10/10   cfg-intf   site-self, reachable
```

Voor alle bekende lokale MAC-adressen die in de database worden weergegeven, wordt de Locator weergegeven.

- Dit is de Locator die moet worden gebruikt om deze vermelding te registreren bij de knooppunt van het controlevlak.
- De 2 MAC-adressen die toebehoorden aan de SVI-Switches worden ook weergegeven, maar worden weergegeven met de markering "niet registreren" die voorkomt dat ze worden geregistreerd.
- Het externe item dat werd gezien in de opdracht mac-adrestabel tonen is geen lokaal MAC-adres en wordt als zodanig niet weergegeven onder de lisp-database.

Voor een Layer 2-instantie worden niet alleen de Layer 2-MAC-adressen als EID geleerd, maar moet ook informatie over de adresresolutie worden geleerd uit ARP- en ND-frames.

- Dit zorgt ervoor dat de LISP VXLAN-structuur deze frames kan doorsturen omdat ze normaal binnen het VLAN worden overstroomd.
- Omdat een Layer 2 Instance-ID niet altijd de mogelijkheid heeft om daar een ander mechanisme te overspoelen waarmee Eindpunten adresoplossingsinformatie voor andere eindpunten in dezelfde instantie kunnen oplossen. Hiervoor leren en registreren de fabric-apparaten deze informatie die lokaal wordt geleerd door Device-Tracking.
- Dit wordt vervolgens ook geregistreerd bij de Control Plane Nodes. Vanwege ND of ARP snuffelen die pakketten worden gepunteerd op de CPU om een verzoek naar de Control Plane knooppunten te activeren om te zien of er een bekend MAC-adres gekoppeld.
- Als een positieve reactie terugkomt, worden de ARP/ND-pakketten herschreven, zodat het MAC-adres van de bestemming wordt gewijzigd van broadcast of multicast naar het MAC-adres van de unicast.
- Dit herschreven pakket kan vervolgens als unicastframe worden doorgestuurd via de LISP VXLAN-fabric.

Als u de informatie over de adresresolutie wilt bekijken die op de switch bekend is, kunt u de opdracht apparaatvolgdatabase weergeven.

- Dit toont alle mappings die bekend zijn door apparaattracking.
- De eigen IP-adressen van de switches worden aangeduid als L(Local) en moeten aanwezig

zijn in de database voor apparaattracking.

Externe vermeldingen worden ook weergegeven in deze uitvoer.

- Als ze worden opgelost nadat het is gesnuffeld de ND of ARP verzoek ze worden geplaatst in de apparaat-tracking database met een Link Layer Adres van 0000.0000.00fd.
- Op het moment dat ze zijn opgelost, wordt de informatie gewijzigd in de richting van het opgeloste mac-adres en wordt de poort gewijzigd in Tu0.

De database voor apparaattracking weergeven

```
<#root>

FE2068#

show device-tracking database vlanid 150


vlanDB has 6 entries for vlan 150, 3 dynamic
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol, DH4 - IPv4 DH
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned
    Network Layer Address                   Link Layer Address     Interface  vlan       prlvl      ag

ARP


172.24.1.3                                0050.5693.8930

        Gi1/0/1    150        0005       31s        REACHABLE  213 s try 0
RMT 172.24.1.4

0050.5693.3120

        Tu0    150        0005       51s        REACHABLE


API


172.24.1.99                               0000.0000.00fd

         Gi1/0/1    150        0000       5s         UNKNOWN   try 0 (25 s)
ND  FE80::1AE4:8804:5B8F:50F6               0050.5693.8930         Gi1/0/1    150        0005       12

ND


2001:DB8::E70B:E8E1:E368:BDB7             0050.5693.8930

         Gi1/0/1    150        0005       137s       REACHABLE  110 s try 0
L   172.24.1.254                            0000.0c9f.f18e         Vl150      150        0100       10
L   2001:DB8::1                             0000.0c9f.f18e         Vl150      150        0100       10
L   FE80::200:CFF:FE9F:F18E                 0000.0c9f.f18e         Vl150      150        0100       10
```

Geef de lokaal geregistreerde toewijzingen weer met de opdracht 'show lisp instance-id <instance> ethernet database address-resolution'

<#root>

```
FE2068#
show lisp instance-id 8191 ethernet database address-resolution

LISP ETR Address Resolution for LISP 0 EID-table Vlan 150 (IID 8191)
(*) -> entry being deleted
Hardware Address       L3 InstID Host Address
0000.0c9f.f18e              4099 FE80::200:CFF:FE9F:F18E/128

                            4099 2001:DB8::1/128

0050.5693.8930              4099 172.24.1.3/32

                            4099 2001:DB8::E70B:E8E1:E368:BDB7/128

                            4099 FE80::1AE4:8804:5B8F:50F6/128
```

1.2 Dynamische IP-adressen leren

Op de fabric-apparaten op een IP-laag wordt een virtueel netwerk gevormd door een LISP Instance-id aan een VRF te koppelen.

- Deze VRF wordt vervolgens geconfigureerd onder de verschillende Switch Virtual Interfaces (SVI) en ze worden onderdeel van het Layer 3 Overlay-netwerk
- In de meeste gevallen behoren deze SVI's ook tot VLAN's die zijn geregistreerd bij hun respectieve Layer 2-instanties.

Zoek de toewijzing tussen VRF en LISP Instance id met de opdracht 'show lisp instance-id <instance> ipv4'

<#root>

```
FE2068#
sh lisp instance-id 4099 ipv4

  Instance ID:                            4099

  Router-lisp ID:                         0
```

```
  Locator table:                          default
  EID table:                              vrf Fabric_VN_1

  Ingress Tunnel Router (ITR):            enabled
  Egress Tunnel Router (ETR):             enabled
  ..
  ITR Map-Resolver(s):                    172.30.250.19


  ETR Map-Server(s):                      172.30.250.19
```

Opmerking: Deze opdracht kan ook worden gebruikt om de verschillende functies te controleren die voor deze instantie kunnen worden ingeschakeld en toont ook de gebruikte Control Plane-knooppunten in de LISP VXLAN-structuur

Zodra een Layer 3-instantie is gemaakt en aan een VRF is gekoppeld, wordt een LISP 0 <instance-id>-interface gemaakt die zichtbaar is in de actieve configuratie en onder show vrf.

- Deze interface hoeft NIET handmatig te worden gemaakt en heeft doorgaans geen configuratie nodig (behalve Multicast Configuration wanneer Underlay Multicast wordt gebruikt).

<#root>

```
FE2068#
show vrf Fabric_VN_1

  Name                              Default RD            Protocols   Interfaces

Fabric_VN_1

                                                          ipv4,ipv6


LI0.4099
```

Vl150

Vl151

In tegenstelling tot Ethernet-frames waarbij alle MAC-adressen in een VLAN worden gebruikt voor IP, moeten IP-adressen binnen een dynamisch EID-bereik worden geleerd.

Een LISP-instantie weergeven

<#root>

FE2068#

sh lisp instance-id 4099 dynamic-eid

LISP Dynamic EID Information for router 0,

IID 4099, EID-table VRF "Fabric_VN_1"

Dynamic-EID name:

Fabric_VN_Subnet_1_IPv4

  Database-mapping EID-prefix: 172.24.1.0/24, locator-set rloc_hosts

  Registering more-specific dynamic-EIDs
  Map-Server(s): none configured, use global Map-Server
  Site-based multicast Map-Notify group: none configured

  Number of roaming dynamic-EIDs discovered: 2

  Last dynamic-EID discovered: 172.24.1.3, 21:17:45 ago

Dynamic-EID name: Fabric_VN_Subnet_1_IPv6

  Database-mapping EID-prefix: 2001:DB8::/64, locator-set rloc_hosts

  Registering more-specific dynamic-EIDs
  Map-Server(s): none configured, use global Map-Server
  Site-based multicast Map-Notify group: none configured

  Number of roaming dynamic-EIDs discovered: 2

Last dynamic-EID discovered: 2001:DB8::E70B:E8E1:E368:BDB7, 21:17:44 ago

Dynamic-EID name: Fabric_VN_Subnet_2_IPv4

Database-mapping EID-prefix: 172.24.2.0/24, locator-set rloc_hosts

Registering more-specific dynamic-EIDs
Map-Server(s): none configured, use global Map-Server
Site-based multicast Map-Notify group: none configured

Number of roaming dynamic-EIDs discovered: 2

Last dynamic-EID discovered: 172.24.2.2, 21:55:56 ago

IP-adressen die zich buiten deze gedefinieerde bereiken bevinden, worden geacht niet in aanmerking te komen voor de verbinding en worden niet in de LISP-databases geplaatst en niet geregistreerd bij de control plane-knooppunten.

<#root>

FE2068#

show lisp instance-id 4099 ipv4 database

LISP ETR IPv4 Mapping Database for LISP 0 EID-table vrf Fabric_VN_1 (IID 4099), LSBs: 0x1
Entries total 4, no-route 0, inactive 0, do-not-register 2

172.24.1.3/32, dynamic-eid Fabric_VN_Subnet_1_IPv4

, inherited from default locator-set rloc_hosts
Uptime: 21:28:51, Last-change: 21:28:51
Domain-ID: local
Service-Insertion: N/A
Locator Pri/Wgt Source State

172.30.250.44

10/10 cfg-intf site-self, reachable

172.24.1.254/32, dynamic-eid Fabric_VN_Subnet_1_IPv4, do not register,

inherited from default locator-set rloc_hosts
Uptime: 22:22:35, Last-change: 22:22:35
Domain-ID: local
Service-Insertion: N/A
Locator Pri/Wgt Source State

172.30.250.44

10/10 cfg-intf site-self, reachable

172.24.2.2/32, dynamic-eid Fabric_VN_Subnet_2_IPv4

, inherited from default locator-set rloc_hosts
  Uptime: 22:07:03, Last-change: 22:07:03
  Domain-ID: local
  Service-Insertion: N/A
  Locator   Pri/Wgt Source   State

172.30.250.44

  10/10   cfg-intf   site-self, reachable

172.24.2.254/32, dynamic-eid Fabric_VN_Subnet_2_IPv4, do not register

, inherited from default locator-set rloc_hosts
  Uptime: 22:22:35, Last-change: 22:22:35
  Domain-ID: local
  Service-Insertion: N/A
  Locator   Pri/Wgt Source   State

172.30.250.44

 10/10   cfg-intf   site-self, reachable

De uitvoer toont alle lokaal bekende IP-adresgegevens.

- Voor hosts zijn dit meestal hostroutes (/32 of /128), maar ze kunnen ook subnetten zijn als deze in de LISP-database op de border node zijn geïmporteerd.
- De IP-adressen van de SVI zelf worden gemarkeerd als "niet registreren". Dit om te voorkomen dat alle fabric-apparaten het IP-adres van Anycast registreren bij de knooppunt van het controlevlak.

<#root>

CP_BN_2071#

sh lisp instance-id 4099 ipv4 database

LISP ETR IPv4 Mapping Database for LISP 0 EID-table vrf Fabric_VN_1 (IID 4099), LSBs: 0x1
Entries total 2, no-route 0, inactive 0, do-not-register 0

0.0.0.0/0

, locator-set rloc_border, auto-discover-rlocs, default-ETR
  Uptime: 2d17h, Last-change: 2d17h
  Domain-ID: local
  Metric: 0
  Service-Insertion: N/A
  Locator   Pri/Wgt Source   State

172.30.250.19

   10/10   cfg-intf   site-self, reachable

10.48.13.0/24, route-import

, inherited from default locator-set rloc_border, auto-discover-rlocs
  Uptime: 2d17h, Last-change: 2d16h
  Domain-ID: local, tag: 65101
  Service-Insertion: N/A
  Locator   Pri/Wgt Source   State

172.30.250.19

   10/10   cfg-intf   site-self, reachable

1.3 Registratie van EID bij het controlevlak

De registratie van eindpunten in een op LISP VXLAN gebaseerde fabric verloopt via een betrouwbare registratie van LISP. Dit betekent dat alle registraties worden gedaan via een gevestigde TCP-sessie, de LISP-sessie. Vanaf elk fabric-apparaat wordt een LISP-sessie ingesteld met elk van de control plane-nodes in de fabric.Via deze LISP-sessie vinden alle registraties plaats. Als er meerdere Control Plane-knooppunten in een stof aanwezig zijn, moeten ze allemaal worden gebruikt om EID's bij te registreren.

De status is Down wanneer er niets te registreren is op het fabric-apparaat, wat normaal gesproken alleen aan de buitengrenzen voorkomt
die geen IP-bereiken registreren bij de knooppunt Control Plane of op Edge-apparaten zonder eindpunt

De registratie van EID gebeurt via LISP Registratie berichten
die worden verzonden naar alle geconfigureerde control plane-nodes.

Als u de LISP-sessie op een fabric-apparaat wilt bekijken, kunt u de opdracht lisp-sessie weergeven gebruiken.
Het toont de staat van de sessie en de tijd dat het is afgelopen.

<#root>

FE2068#

show lisp session

Sessions for VRF default, total: 1, established: 1
Peer   State   Up/Down   In/Out   Users

172.30.250.19:4342   **Up**

        22:06:07   9791/6531   10

De LISP-sessie die als Omlaag wordt weergegeven, kan plaatsvinden op apparaten die geen EID

hebben om zich te registreren bij de knoop van het regelvlak.
Doorgaans zijn dat randknooppunten die geen routes importeren in de fabric of Edge-apparaten zonder dat er eindpunten zijn aangesloten.

Geef meer gedetailleerde informatie over een LISP-sessie weer met de opdracht 'show lisp session vrf default <ip address>'

<#root>

FE2068#

show lisp vrf default session 172.30.250.19

Peer address: 172.30.250.19:4342
Local address: 172.30.250.44:13255
Session Type:

Active

Session State:

Up

(22:07:24)
Messages in/out: 9800/6537
Bytes in/out: 616771/757326
Fatal errors: 0
Rcvd unsupported: 0
Rcvd invalid VRF: 0
Rcvd override: 0
Rcvd malformed: 0
Sent deferred: 1
SSO redundancy: N/A
Auth Type: None
Accepting Users: 0
Users: 10

Type	ID	In/Out	State
Policy subscription	lisp 0 IID 4099 AFI IPv4	2/1	Established
Pubsub subscriber	lisp 0 IID 4099 AFI IPv6	1/0	Idle
Pubsub subscriber	lisp 0 IID 8191 AFI MAC	2/0	Idle
Pubsub subscriber	lisp 0 IID 8192 AFI MAC	0/0	Idle

ETR Reliable Registration lisp 0 IID 4099 AFI IPv4

6/5 TCP

ETR Reliable Registration lisp 0 IID 4099 AFI IPv6

1/3 TCP

ETR Reliable Registration lisp 0 IID 8191 AFI MAC

9769/6517 TCP

ETR Reliable Registration lisp 0 IID 8192 AFI MAC

```
           2/6      TCP
  ETR Reliable Registration lisp 0 IID 16777214 AFI IPv4            4/4      TCP
  Capability Exchange       N/A                                     1/1      waiting
```

Deze gedetailleerde uitvoer van de sessie laat zien welke Instanties actief zijn met EID die zijn geregistreerd bij de knooppunten van het controlevlak.

<#root>

CP_BN_2071#

show lisp session

```
Sessions for VRF default, total: 7, established: 4
Peer                          State      Up/Down        In/Out    Users
```

172.30.250.19:4342 **Up**

22:10:52 1198618/1198592 4

172.30.250.19:49270 **Up**

22:10:52 1198592/1198618 3

172.30.250.30:25780 **Up**

22:10:38 6534/9805 6

172.30.250.44:13255 **Up**

22:10:44 6550/9820 7

Wanneer men kijkt naar het aantal sessies op een Control Plane node, worden meestal meer sessies weergegeven die omhoog staan.

- Als dit een gecoloceerde Border/CP-node is, is er ook een LISP-sessie naar zichzelf toe ingesteld.
- In dit geval is er een sessie van 172.30.250.19:4342 tot 172.30.250.19:49270.
- Via deze sessie registreert de Border-component zijn EID met de Control Plane Node.

1.4 Informatie over het bedieningsvlak

Met de informatie die wordt verstrekt door de Fabric Devices via registratie, kan de knooppunt van het besturingsvlak een volledig beeld van de fabric maken. Per Instance-id onderhoudt het een tabel met de geleerde EID's en de bijbehorende Routing Locators.

Geef dit weer voor de Layer 3-instanties op de site met opdracht lisp tonen

<#root>

CP_BN_2071#

```
show lisp site


LISP Site Registration Information
* = Some locators are down or unreachable
# = Some registrations are sourced by reliable transport
Site Name      Last      Up     Who Last             Inst     EID Prefix
               Register         Registered           ID
site_uci       never     no     --                   4097     0.0.0.0/0
               never     no     --                   4097     172.23.255.0/24
               never     no     --                   4097     172.24.255.0/24
               never     no     --                   4099     0.0.0.0/0
               00:00:00

yes#   172.30.250.19:49270  4099     10.48.13.0/24


               never     no     --                   4099     172.23.1.0/24
               never     no     --                   4099     172.24.1.0/24
               21:35:06

yes#   172.30.250.44:13255  4099     172.24.1.3/32


               22:11:46

yes#   172.30.250.30:25780  4099     172.24.1.4/32


               never     no     --                   4099     172.24.2.0/24
               22:11:52

yes#   172.30.250.44:13255  4099     172.24.2.2/32
```

Deze opdracht toont alle geregistreerde EID en de laatste die de EID heeft geregistreerd. Het is belangrijk op te merken dat dit meestal ook de RLOC is die in gebruik is, maar dit kan verschillen. Ook EID's kunnen worden geregistreerd bij meerdere RLOC's.

Als u de volledige details wilt weergeven, bevat de opdracht de EID en de instantie

<#root>

```
CP_BN_2071#

show lisp site 172.24.1.3/32 instance-id 4099


LISP Site Registration Information
Site name: site_uci
Description: map-server
Allowed configured locators: any
Requested EID-prefix:
  EID-prefix:

172.24.1.3/32 instance-id 4099


    First registered:     21:35:53
    Last registered:      21:35:53
    Routing table tag:    0
```

```
    Origin:               Dynamic, more specific of 172.24.1.0/24
    Merge active:         No
    Proxy reply:
```

Yes

```
    Skip Publication:     No
    Force Withdraw:       No
    TTL:
```

1d00h

```
    State:
```

complete

```
    Extranet IID:         Unspecified
    Registration errors:
      Authentication failures:   0
      Allowed locators mismatch: 0
    ETR 172.30.250.44:13255, last registered 21:35:53, proxy-reply, map-notify
                             TTL 1d00h, no merge, hash-function sha1
                             state complete, no security-capability
                             nonce 0x6ED7000E-0xD4C608C5
                             xTR-ID 0x88F15053-0x40C0253D-0xAE5EA874-0x2551DB71
                             site-ID unspecified
                             Domain-ID local
                             Multihoming-ID unspecified
                             sourced by reliable transport
      Locator        Local  State      Pri/Wgt  Scope
```

172.30.250.44 yes   up

```
          10/10   IPv4 none
```

Opmerking: in gedetailleerde uitvoer zijn een paar dingen belangrijk om op te letten:

- Proxy, met deze set reageert de Control Plane node direct op een Map-request. In traditionele LISP wordt een kaartverzoek doorgestuurd naar de XTR die de EID registreerde, maar met Proxy-set reageert de control plane node direct
- TTL, dit is de Time To Live van de EID registratie. Standaard is dit 24 uur
- ETR-informatie, dit heeft betrekking op het weefselapparaat dat de EID-registratie heeft verzonden
- RLOC-informatie, dit is de RLOC die moet worden gebruikt om de EID te bereiken. Dit bevat ook statusinformatie zoals in omhoog/omlaag. als de RLOC omlaag is, wordt deze niet gebruikt. Het bevat ook een gewicht en prioriteit die kunnen worden gebruikt wanneer er meerdere RLOC's bestaan voor een EID om de voorkeur te geven aan een van hen.

Als u de registratiegeschiedenis op de knooppunt Control Plane wilt bekijken, wordt de

registratiegeschiedenis van de lisp-server weergegeven.

- Het geeft een overzicht van EID's die zijn geregistreerd en uitgeschreven.

Registratiegeschiedenis weergeven

<#root>

```
CP_BN_2071#
```

show lisp server registration-history last 10

```
Map-Server registration history
Roam = Did host move to a new location?
WLC = Did registration come from a Wireless Controller?
Prefix qualifier: + = Register Event, - = Deregister Event, * = AR register event
Timestamp (UTC)      Instance Proto Roam WLC Source
                                            EID prefix / Locator
*Mar 24 20:49:51.490     4099 TCP   No   No  172.30.250.19
                                          + 10.48.13.0/24
*Mar 24 20:49:51.491     4099 TCP   No   No  172.30.250.19
                                          - 10.48.13.0/24
*Mar 24 20:49:51.621     4099 TCP   No   No  172.30.250.19
                                          + 10.48.13.0/24
*Mar 24 20:49:51.622     4099 TCP   No   No  172.30.250.19
                                          - 10.48.13.0/24
*Mar 24 20:49:51.752     4099 TCP   No   No  172.30.250.19
                                          + 10.48.13.0/24
*Mar 24 20:49:51.754     4099 TCP   No   No  172.30.250.19
                                          - 10.48.13.0/24
*Mar 24 20:49:51.884     4099 TCP   No   No  172.30.250.19
                                          + 10.48.13.0/24
*Mar 24 20:49:51.886     4099 TCP   No   No  172.30.250.19
                                          - 10.48.13.0/24
*Mar 24 20:49:52.017     4099 TCP   No   No  172.30.250.19
                                          + 10.48.13.0/24
*Mar 24 20:49:52.019     4099 TCP   No   No  172.30.250.19
                                          - 10.48.13.0/24
```

Geef de geregistreerde EID voor Ethernet weer met de opdracht show lisp instance-id <instance> ethernetserver (Dit geeft een vergelijkbare uitvoer als voor Layer 3)

<#root>

```
CP_BN_2071#
```

show lisp instance-id 8191 ethernet server

```
LISP Site Registration Information
* = Some locators are down or unreachable
# = Some registrations are sourced by reliable transport
Site Name      Last      Up     Who Last             Inst     EID Prefix
               Register         Registered           ID
site_uci       never     no     --                   8191     any-mac
```

```
              00:00:04
yes#   172.30.250.44:13255  8191     0019.3052.6d7f/48

              21:36:41
yes#   172.30.250.44:13255  8191     0050.5693.8930/48

              22:13:20
yes#   172.30.250.30:25780  8191     0050.5693.f1b2/48
```

Voeg het MAC-adres toe voor meer gedetailleerde informatie over een registratie

<#root>

```
CP_BN_2071#
show lisp instance-id 8191 ethernet server 0019.3052.6d7f


LISP Site Registration Information
Site name: site_uci
Description: map-server
Allowed configured locators: any
Requested EID-prefix:
  EID-prefix:
0019.3052.6d7f/48 instance-id 8191


    First registered:     22:14:38
    Last registered:      00:00:03
    Routing table tag:    0
    Origin:               Dynamic, more specific of any-mac
    Merge active:         No
    Proxy reply:
Yes


    Skip Publication:     No
    Force Withdraw:       No
    TTL:
1d00h


    State:
complete


    Extranet IID:         Unspecified
    Registration errors:
      Authentication failures:   0
      Allowed locators mismatch: 0
    ETR 172.30.250.30:25780, last registered 00:00:03, proxy-reply, map-notify
                             TTL 1d00h, no merge, hash-function sha1
```

```
                            state complete, no security-capability
                            nonce 0x0465A327-0xA3A2974C
                            xTR-ID 0x280403CF-0x598BAAF1-0x3E70CE52-0xE8F09E6E
                            site-ID unspecified
                            Domain-ID local
                            Multihoming-ID unspecified
                            sourced by reliable transport
      Locator         Local  State      Pri/Wgt  Scope
```

172.30.250.30 yes

```
   up           10/10   IPv4 none
```

Voeg 'registratiegeschiedenis' toe om de registratiegeschiedenis voor ethernet-EID te bekijken

---

Opmerking: Deze opdracht is erg handig wanneer apparaten in de verbinding zwerven om te zien waar en wanneer het MAC-adres is geregistreerd

---

<#root>

CP_BN_2071#

show lisp instance-id 8191 ethernet server registration-history

```
Map-Server registration history
Roam = Did host move to a new location?
WLC = Did registration come from a Wireless Controller?
Prefix qualifier: + = Register Event, - = Deregister Event, * = AR register event
Timestamp (UTC)      Instance Proto Roam WLC Source
                                            EID prefix / Locator
*Mar 24 20:47:10.291     8191 TCP   Yes  No  172.30.250.44
                                          + 0019.3052.6d7f/48
*Mar 24 20:47:10.296     8191 TCP   No   No  172.30.250.30
                                          - 0019.3052.6d7f/48
*Mar 24 20:47:18.644     8191 TCP   Yes  No  172.30.250.30
                                          + 0019.3052.6d7f/48
*Mar 24 20:47:18.647     8191 TCP   No   No  172.30.250.44
                                          - 0019.3052.6d7f/48
*Mar 24 20:47:20.700     8191 TCP   Yes  No  172.30.250.44
                                          + 0019.3052.6d7f/48
*Mar 24 20:47:20.702     8191 TCP   No   No  172.30.250.30
                                          - 0019.3052.6d7f/48
*Mar 24 20:47:31.914     8191 TCP   Yes  No  172.30.250.30
                                          + 0019.3052.6d7f/48
*Mar 24 20:47:31.918     8191 TCP   No   No  172.30.250.44
                                          - 0019.3052.6d7f/48
*Mar 24 20:47:40.206     8191 TCP   Yes  No  172.30.250.44
                                          + 0019.3052.6d7f/48
*Mar 24 20:47:40.210     8191 TCP   No   No  172.30.250.30
                                          - 0019.3052.6d7f/48
```

Om de geregistreerde adresoplossingsinformatie op de knooppunt van het regelvlak te bekijken,

wordt de opdracht toegevoegd met adresresolutie.

- Dit toont alleen de toewijzingen tussen het MAC-adres en hun Layer 3-informatie en moet voornamelijk worden gebruikt voor de Fabric Edges om de Layer 2-bestemmings-MAC-adressen van broadcast / multicast naar unicast te herschrijven.
- Het RLOC dat overeenkomt met dat Layer 2 MAC-adres zou afzonderlijk worden opgelost.

Voeg 'address-resolution' toe om de geregistreerde adresoplossingsinformatie op de knooppunt Control Plane te zien

<#root>

```
CP_BN_2071#
sh lisp instance-id 8191 ethernet server address-resolution

Address-resolution data for router lisp 0 instance-id 8191
L3 InstID    Host Address                                Hardware Address

4099    172.24.1.3/32                                0050.5693.8930

     4099    172.24.1.4/32                                0050.5693.f1b2

     4099    2001:DB8::E70B:E8E1:E368:BDB7/128            0050.5693.8930

     4099    2001:DB8::F304:BCCD:6BF3:BFAF/128            0050.5693.f1b2

     4099    FE80::3EE:5111:BA77:E37D/128                 0050.5693.f1b2

     4099    FE80::1AE4:8804:5B8F:50F6/128                0050.5693.8930
```

Opmerking: Hoewel de lokale IPv6-adressen van de koppeling niet overeenkomen met de IPv6 Dynamic EID, moeten ze worden geleerd voor adresresolutie en zou dit worden weergegeven op de knooppunt Control Plane. Deze worden niet zelf geregistreerd onder de Layer 3 Instance ID, maar zijn beschikbaar voor Adresresolutie.

Externe bestemmingen oplossen

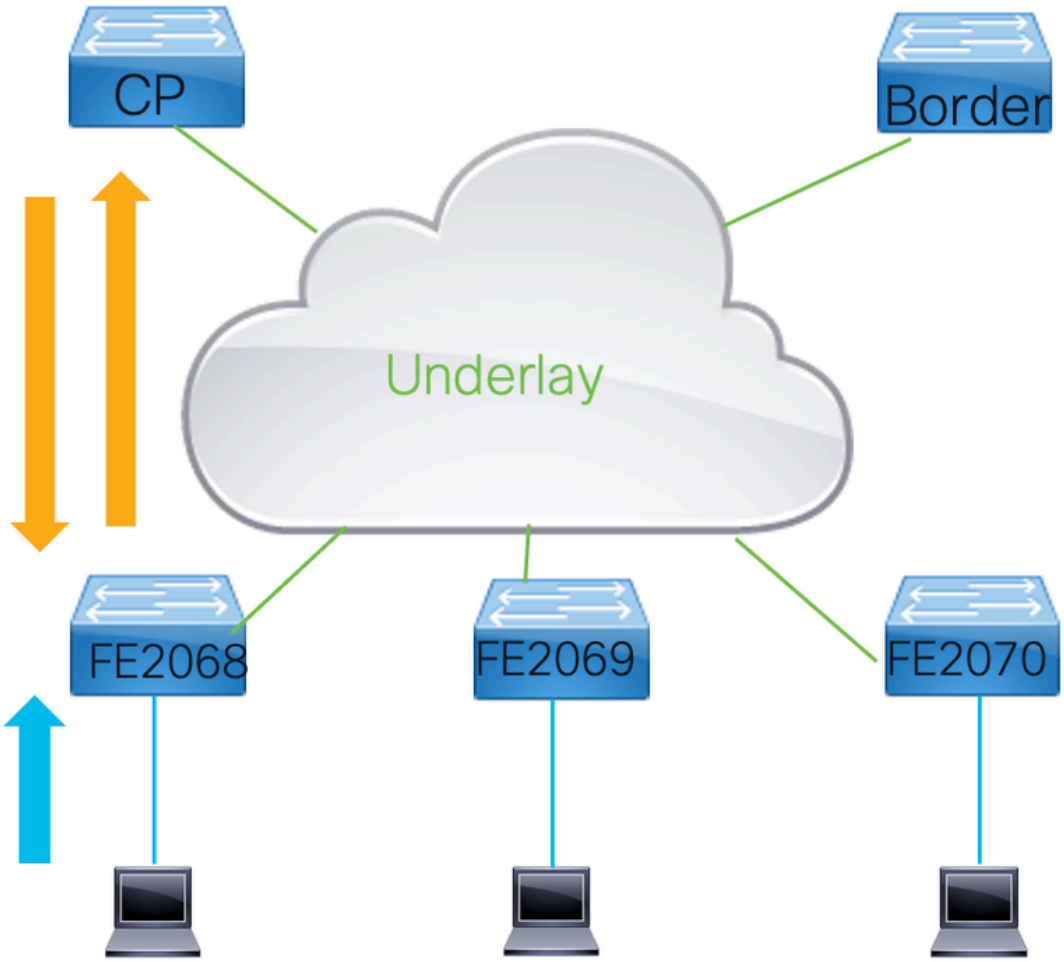
Voor het doorsturen van verkeer via een LISP VXLAN-fabric moet de RLOC van een bestemming worden opgelost. Binnen een LISP VXLAN-fabric wordt dit gedaan met behulp van een kaartcache waaruit informatie wordt geplaatst in de Forwarding Information Base (FIB) van het Fabric-apparaat.

Met LISP VXLAN-verbindingen moeten kaartcaches worden geactiveerd als gevolg van gegevenssignalen.

- Dit betekent dat het verkeer wordt doorgestuurd naar de CPU en de CPU maakt een kaartverzoek naar de Control Plane-node om te zoeken naar de RLOC-informatie waarnaar frames naar dat EID moeten worden verzonden.
- Het controleplan zou, wanneer het een verzoek om een kaart ontvangt, ofwel de routing locator-informatie verstrekken die aan deze EID is gekoppeld, ofwel een negatief antwoord op de kaart terugsturen.
- Wanneer het een negatief kaartantwoord verzendt, zou het knooppunt van het controlevlak niet alleen aangeven dat de gevraagde EID niet bekend is, maar zou het het volledige blok EID's aanbieden waartoe deze EID zou behoren en waarvoor het geen registratie zou hebben.

Met de informatie in de map-antwoord van de control plane node wordt de map-cache bijgewerkt.

- De TTL voor kaartreacties is meestal 24 uur. (Voor negatieve kaartreacties is dit meestal slechts 15 minuten).
- Voor Ethernet EID worden de negatieve kaartantwoorden niet in de kaartcache geplaatst. (Dit wordt alleen gedaan voor Layer 3 Instances).



2.1 Ethernet-kaartcache

Geef de Ethernet map-cache weer met de opdracht lisp instance-id <instance> map-cache weergeven

<#root>

FE2067#

show lisp instance-id 8191 ethernet map-cache

LISP MAC Mapping Cache for LISP 0 EID-table

Vlan 150 (IID 8191)

, 1 entries
0

019.3052.6d7f/48

, uptime: 00:00:07, expires: 23:59:52, via map-reply, complete
  Locator   Uptime   State Pri/Wgt   Encap-IID

172.30.250.44

```
00:00:07  up      10/10        -
```

Deze opdracht toont de vermelding van het externe MAC-adres die zou zijn opgelost.

- Om een kaartcachevermelding voor een Ethernet-instantie te activeren, moet het verkeer naar een onbekende bestemming worden verzonden.
- Dat zou resulteren in het Fabric Device om te proberen het op te lossen via LISP.
- Zodra het via een kaart-antwoord is geleerd, zou het in de kaartcache worden geplaatst en de volgende frames naar die laag 2-bestemming zouden rechtstreeks naar de geleerde Routing Locator worden verzonden.

Optioneel in Layer 2 Instances is het gebruik van overstroming van BUM verkeer.

- LISP/VXLAN overspoelt het verkeer niet standaard, omdat het een overlay-technologie gebruikt, maar een IP Multicast-groep kan worden geconfigureerd in het onderliggende netwerk (GRT) waardoor laag 2-frames kunnen worden overspoeld.

Het adres van de onderliggende uitzendgroep weergeven

<#root>

```
FE2068#
sh run | sec instance-id 8191


 instance-id 8191
  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 150


broadcast-underlay 239.0.1.19


   database-mapping mac locator-set rloc_hosts
   exit-service-ethernet
  !
  exit-instance-id
```

2.2 IP-kaartcache

Voor Layer 3 instanties is de kaart-cache informatie vergelijkbaar met ethernet build by traffic naar de CPU te sturen signaal veroorzaakt een kaart-verzoek te worden verzonden.

- Echter, voor Layer 3 pakketten alleen krijgen punted naar CPU om te signaleren wanneer dit moet worden ingesteld. Dit wordt gedaan met de opdracht map-cache die is geconfigureerd. Voor IPv4 is dit 0.0.0.0/0 en ::0/0 voor IPv6.
- De configuratie van deze kaartcacheinvoer op de grensknooppunten moet zorgvuldig gebeuren. Als een border node is geconfigureerd met deze map-cache 0.0.0.0/0 of ::0/0

map-cache entry, probeert deze onbekende bestemmingen op te lossen via de fabric in plaats van deze buiten de fabric te routeren.

De kaartcacheconfiguratie weergeven

<#root>

```
FE2068#
sh run | sec instance-id 4099


 instance-id 4099
  remote-rloc-probe on-route-change
  dynamic-eid Fabric_VN_Subnet_1_IPv4
   database-mapping 172.24.1.0/24 locator-set rloc_hosts
   exit-dynamic-eid
  !
  dynamic-eid Fabric_VN_Subnet_1_IPv6
   database-mapping 2001:DB8::/64 locator-set rloc_hosts
   exit-dynamic-eid
  !
  service ipv4
   eid-table vrf Fabric_VN_1


map-cache 0.0.0.0/0 map-request


   exit-service-ipv4
  !
  service ipv6
   eid-table vrf Fabric_VN_1
   map-cache ::/0 map-request


   exit-service-ipv6
  !
  exit-instance-id
```

De map-cache 0.0.0.0/0 en ::/0 map-request zorgen ervoor dat een map-cache item geconfigureerd wordt in de map-cache met de "send-map-request" acties. Verkeer dat dit raakt, activeert kaartaanvragen. Aangezien de map-cache-items in de FIB moeten worden geplaatst die werkt op basis van de langste overeenkomst, wordt dit toegepast op al het gerouteerde IP-verkeer dat geen van de meer specifieke items raakt.

- Op ondersteunde platforms om te voorkomen dat het eerste pakket wordt gedropt, wordt de actie send-map-request + encapsulate naar proxy ETR weergegeven.
  Dit leidt ertoe dat het eerste pakket naar een onbekende bestemming een kaartverzoek activeert en dat het pakket wordt doorgestuurd naar de proxy-eter indien aanwezig.

<#root>

```
FE2067#
```

show lisp instance-id 4099 ipv4 map-cache

LISP IPv4 Mapping Cache for LISP 0 EID-table vrf Fabric_VN_1 (IID 4099), 6 entries

0.0.0.0/0,

uptime: 22:28:18, expires: 00:13:41, via map-reply, unknown-eid-forward
action:

send-map-request + Encapsulating to proxy ETR

PETR	Uptime	State	Pri/Wgt	Encap-IID	Metric
172.30.250.19	22:28:18	up	10/10	-	0

10.48.13.0/24,

uptime: 02:31:26, expires: 21:28:34, via map-reply, complete

Locator	Uptime	State	Pri/Wgt	Encap-IID
172.30.250.19				
	02:31:26	up	10/10	-

172.24.1.0/24

, uptime: 22:31:34, expires: never, via dynamic-EID, send-map-request

Negative cache entry, action: send-map-request

172.24.2.0/24

, uptime: 22:31:34, expires: never, via dynamic-EID, send-map-request

Negative cache entry, action: send-map-request

172.24.2.2/32

, uptime: 00:00:21, expires: 23:59:38,

via map-reply, complet

e

Locator	Uptime	State	Pri/Wgt	Encap-IID
172.30.250.44				
	00:00:21	up	10/10	-

172.28.0.0/14,

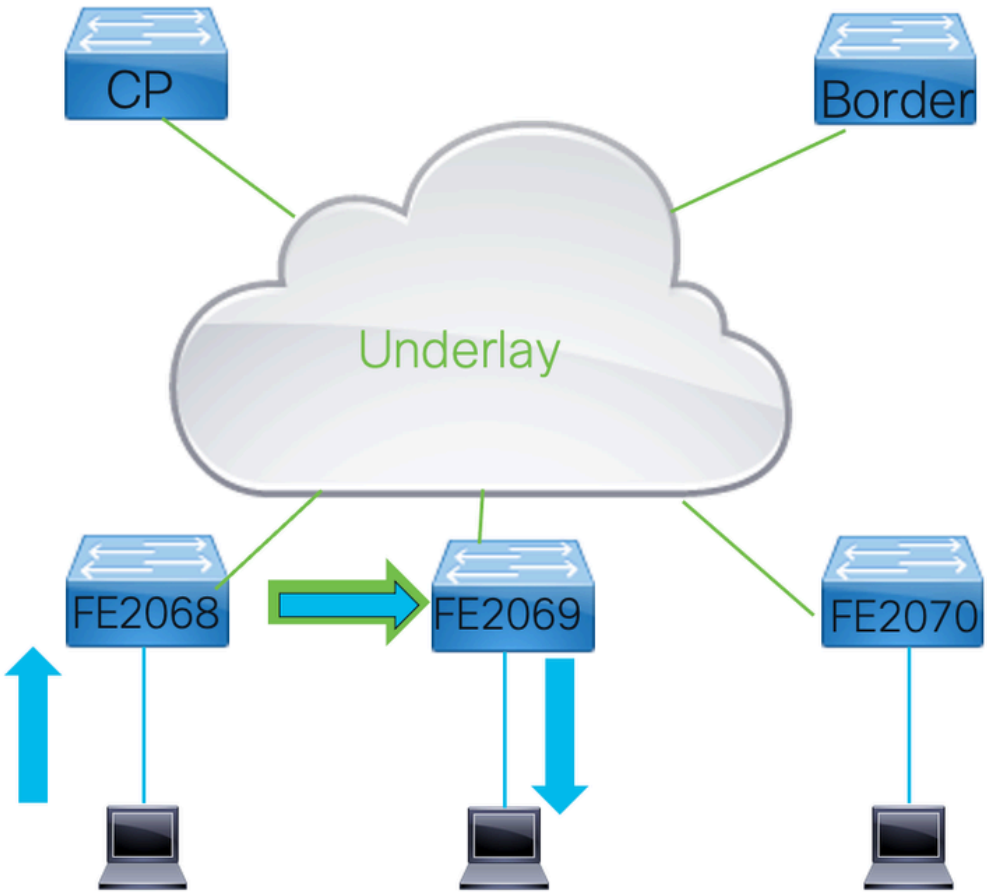
uptime: 22:28:22, expires: 00:13:39, via map-reply, unknown-eid-forward

PETR	Uptime	State	Pri/Wgt	Encap-IID	Metric
172.30.250.19					
	22:28:19	up	10/10	-	0

In deze output worden een paar items getoond.

- 10.48.13.0/24 en 172.24.2.2/32 in deze uitvoer wordt geleerd via map-reply en zijn voltooid. Het verkeer naar die bestemmingen moet worden ingekapseld en doorgestuurd naar de respectieve locaties.
- De 172.28.0.0/14 is een voorbeeld van een negatief kaartantwoord dat is ontvangen en een blok IP-adressen dat is geretourneerd. Verkeer naar dit subnet leidt niet tot een kaartverzoek zolang dit item zich in de kaartcache bevindt.

Verkeer doorsturen via de verbinding



3.1 Layer 2 of Layer 3 Forwarding

Verkeer in een LISP/VXLAN-fabric kan worden doorgestuurd via Layer 2- of Layer Instances.

- De bepaling welke instantie wordt gebruikt, is afhankelijk van het MAC-adres van de bestemming van de frames.
- Frames die naar een ander MAC-adres worden verzonden dan degene die is geregistreerd bij de switch die het frame moet doorsturen, moeten Layer 2 gebruiken. Als het pakket bestemd is voor de switch, wordt het doorgestuurd via Layer 3.

- Dit is dezelfde logica die van toepassing zou zijn op normaal doorsturen via een Catalyst 9000-serie switch.

3.2 Layer 2 Forwarding

Layer 2 doorsturen via een LISP VXLAN-fabric gebeurt op basis van het MAC-adres van de Layer 2-bestemming. Externe bestemmingen worden ingevoegd in de MAC-adrestabel met uitgang-interface L2LI0.

De lokale en externe laag 2-interfaces weergeven

<#root>

```
FE2068#
```

show mac address-table vlan 150

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 150    0000.0c9f.f18e    STATIC      Vl150
 150    0050.5693.8930    DYNAMIC     Gi1/0/1
 150    2416.9db4.33fd    STATIC      Vl150
```

<- Local

```
 150    0019.3052.6d7f    CP_LEARN
```

L2LI0 <- Remote

```
Total Mac Addresses for this criterion: 3
Total Mac Addresses installed by LISP: REMOTE: 1
```

Voor onbekende bestemmingen wordt, indien geconfigureerd, verkeer verzonden via de geconfigureerde IP Multicast-groep in de onderlaag.

- Om een correcte doorstroming van uitzendingen, Unknown Unicast en Multicast (Selective Multicast flood only) verkeer te garanderen, is een correct werkende multicast-omgeving in de onderlaag nodig.
- Het verkeer dat via deze multicast-onderleggroep zou worden verzonden, moet worden ingekapseld in VXLAN.
- Alle andere randen moeten lid worden van de multicast-groep en verkeer ontvangen en het verkeer voor bekende Layer 2-instanties decapsuleren.

De onderliggende IP Multicast-groep weergeven

<#root>

```
FE2068#
```

sh ip mroute 239.0.19.1

```
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route,
       x - VxLAN group, c - PFP-SA cache created entry,
       * - determined by Assert, # - iif-starg configured on rpf intf,
       e - encap-helper tunnel flag, l - LISP decap ref count contributor
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
                          t - LISP transit group
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 239.0.1.19), 00:02:36/stopped, RP 172.31.255.1, flags: SJCF
  Incoming interface: GigabitEthernet1/0/23, RPF nbr 172.30.250.42
  Outgoing interface list:
    L2LISP0.8191, Forward/Sparse-Dense, 00:02:35/00:00:24, flags:
(
```

172.30.250.44, 239.0.1.19

```
), 00:02:03/00:00:56, flags: FT
  Incoming interface:
```

Null0

```
, RPF nbr 0.0.0.0
  Outgoing interface list:
```

GigabitEthernet1/0/23

```
, Forward/Sparse, 00:02:03/00:03:23, flags:
(
```

172.30.250.30, 239.0.1.19

```
), 00:02:29/00:00:30, flags: JT
  Incoming interface:
```

GigabitEthernet1/0/23

```
, RPF nbr 172.30.250.42
  Outgoing interface list:
```

L2LISP0.8191

```
, Forward/Sparse-Dense, 00:02:29/00:00:30, flags:
```

Deze uitvoer toont een S-, G-vermelding voor alle andere randen in de fabric waarin clients zijn geconfigureerd die overstroomd verkeer zouden verzenden. Het toont ook een S, G-vermelding

met de Loopback0 van dit Edge-apparaat als bron.

Voor de ontvangstzijde van het verkeer door de onderliggende multicastgroep toont de opdracht show ip mroute ook de L2LISP0.<instance>
dit zou aangeven voor welke Layer 2 Instances dit randapparaat zou worden gedecapsuleerd en overstroomd verkeer zou doorsturen naar zijn
relevante interfaces.

3.3 Layer 3-forwardinginformatie

Om te bepalen hoe verkeer wordt doorgestuurd wanneer een LISP VXLAN-fabric wordt geïmplementeerd, is het belangrijk om CEF te verifiëren.

- LISP voegt, in tegenstelling tot traditionele routeringsprotocollen, de routeringsrichting niet in de routeringstabel in, maar werkt rechtstreeks samen met CEF om de FIB bij te werken.

Voor een bepaalde externe bestemming bevat de kaartcachegegevens de locatiegegevens die moeten worden gebruikt.

De locatiegegevens weergeven

<#root>

```
FE2067#
sh lisp instance-id 4099 ipv4 map-cache 172.24.2.2

LISP IPv4 Mapping Cache for LISP 0 EID-table vrf Fabric_VN_1 (IID 4099), 1 entries

172.24.2.2/32
, uptime: 11:19:02, expires: 12:40:57, via map-reply, complete
  Sources: map-reply
  State: complete, last modified: 11:19:02, map-source: 172.30.250.44
  Idle, Packets out: 2(1152 bytes), counters are not accurate (~ 11:18:35 ago)
  Encapsulating dynamic-EID traffic
  Locator        Uptime    State  Pri/Wgt     Encap-IID

172.30.250.44
  11:19:02  up      10/10        -
    Last up-down state change:         11:19:02, state change count: 1
    Last route reachability change:    11:19:02, state change count: 1
    Last priority / weight change:     never/never
    RLOC-probing loc-status algorithm:
      Last RLOC-probe sent:            11:19:02 (rtt 2ms)
```

Vanuit de map-cache is de Locator die voor deze EID wordt gebruikt 172.30.250.44. Dus verkeer naar deze bestemming moet worden ingekapseld en de buitenste IP-header heeft een IP-

bestemmingsadres van 172.30.250.44.

In de routeringstabel voor de VRF die in dit geval wordt gebruikt, wordt dit item niet weergegeven.

<#root>

FE2067#

show ip route vrf Fabric_VN_1

```
Routing Table: Fabric_VN_1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected
Gateway of last resort is not set
      172.24.0.0/16 is variably subnetted, 5 subnets, 2 masks
C        172.24.1.0/24 is directly connected, Vlan150
l        172.24.1.4/32 [10/1] via 172.24.1.4, 06:11:02, Vlan150
L        172.24.1.254/32 is directly connected, Vlan150
C        172.24.2.0/24 is directly connected, Vlan151
L        172.24.2.254/32 is directly connected, Vlan151
```

CEF-uitgangen geven meer informatie over het doorsturen via de LISP VXLAN-fabric.

- Wanneer het detailtrefwoord aan de opdracht show ip cef wordt toegevoegd, geeft dit niet alleen de bestemming voor het ingekapselde frame dat moet worden verzonden.
- De interface van Egress met deze uitvoer is LISP 0.<instance> geeft aan dat het verkeer ingekapseld wordt verzonden.

<#root>

FE2067#

sh ip cef vrf Fabric_VN_1 172.24.2.2 detail

```
172.24.2.2/32, epoch 1, flags [subtree context, check lisp eligibility]
  SC owned,sourced: LISP remote EID - locator status bits 0x00000001
  LISP remote EID: 2 packets 1152 bytes
```

fwd action encap

```
, dynamic EID need encap
  SC inherited: LISP cfg dyn-EID - LISP configured dynamic-EID
  LISP EID attributes: localEID No, c-dynEID Yes, d-dynEID No, a-dynEID No
  SC inherited: LISP generalised SMR - [enabled, inheriting, 0x7FF95B3E0BE8 locks: 5]
```

```
  LISP source path list

nexthop 172.30.250.44 LISP0.4099

  2 IPL sources [no flags]

nexthop 172.30.250.44 LISP0.4099
```

Aangezien het verkeer ingekapseld naar de volgende hop wordt verzonden, is de volgende stap om een show ip cef <next hop> uit te voeren om de uitgang-interface te zien waar het pakket ook zou worden gerouteerd.

Uitvoeren om de uitgang-interface te bekijken

<#root>

```
FE2067#

sh ip cef 172.30.250.44

172.30.250.44/32

nexthop 172.30.250.38 GigabitEthernet1/0/23
```

Opmerking: Er zijn 2 verschillende niveaus van Equal Cost Multiple Path (ECMP)-routering mogelijk.

- Het verkeer kan in de overlay worden verdeeld in de belasting als er 2 geadverteerde RLOC's zijn en de belasting in het onderliggende netwerk kan worden verdeeld als er redundante paden bestaan om een RLOC IP-adres te bereiken.
- Aangezien de UDP-bestemmingspoort is vastgesteld op 4789 en de bron- en bestemmings-IP-adressen voor alle stromen tussen twee fabric-apparaten hetzelfde zijn, moet een of andere vorm van antipolarisatiemechanisme plaatsvinden om te voorkomen dat alle pakketten over hetzelfde pad worden gerouteerd.
- Met LISP VXLAN is dit de UDP-bronpoort in de buitenste header die anders zou zijn voor verschillende stromen in het overloopnetwerk.

3.4 Pakketformaat

- Binnen LISP VXLAN-fabrics is al het verkeer volledig ingekapseld in VXLAN. Dit omvat het volledige Layer 2-frame om zowel Layer 2- als Layer 3-overlays te kunnen ondersteunen.

Voor Layer 2-frames is de oorspronkelijke koptekst ingekapseld. Voor frames die via een Layer 3-instantie worden verzonden, wordt een dummy Layer 2-koptekst gebruikt.

<#root>

```
Ethernet II, Src: 24:16:9d:3d:56:67 (24:16:9d:3d:56:67), Dst: 6c:31:0e:f6:21:c7 (6c:31:0e:f6:21:c7)
 Internet Protocol Version 4, Src: 172.30.250.30, Dst: 172.30.250.44
  User Datagram Protocol, Src Port: 65288, Dst Port: 4789
   Virtual eXtensible Local Area Network
   Flags: 0x8800, GBP Extension, VXLAN Network ID (VNI)
   1... .... .... .... = GBP Extension: Defined
   .... .... .0.. .... = Don't Learn: False
   .... 1... .... .... = VXLAN Network ID (VNI): True
   .... .... .... 0... = Policy Applied: False
   .000 .000 0.00 .000 = Reserved(R): 0x0000

   Group Policy ID: 16


   VXLAN Network Identifier (VNI): 4099


   Reserved: 0
    Ethernet II, Src: 00:00:00:00:80:a3 (00:00:00:00:80:a3), Dst: ba:25:cd:f4:ad:38 (ba:25:cd:f4:ad:38)
     Internet Protocol Version 4, Src: 172.24.1.4, Dst: 172.24.2.2
      Internet Control Message Protocol
```

Zoals te zien is aan de monsteropname van een frame dat door een LISP VXLAN-fabric wordt gedragen, bevindt zich het volledig ingekapselde frame in het vxlan-pakket. Omdat het een laag 3-frame is, is de ethernetheader een dummy-header.

In de VXLAN-header bevat het veld VLAN Network Identifier de LISP-instantie-id waarvan het frame ook deel uitmaakt.

- Via het veld Groepsbeleid-ID wordt de SGT-tag van het frame uitgevoerd.
- Dit wordt ingesteld op het binnendringen in de structuur en doorgezet naar de structuur totdat op groepen gebaseerde beleidshandhaving moet worden uitgevoerd.

Authenticatie en handhaving van beveiliging

4.1 Switch-poortverificatie

Om dynamisch eindpunten aan hun respectieve VLAN's toe te wijzen en ze een SGT-tagverificatie toe te wijzen, kan worden gebruikt.

- Verificatieprotocollen als Dot1x/MAB/central webauth kunnen worden geïmplementeerd om gebruikers en eindpunten te verifiëren en te autoriseren op een Radius-server die attributen terugstuurt naar de switch om netwerktoegang tot de client/het eindpunt in de juiste pool en met de juiste netwerktoegangsautorisatie mogelijk te maken.

Voor LISP VXLAN-fabric zijn er weinig gemeenschappelijke radius-attributen:

- Vlan-toewijzing: deze kenmerken worden ingesteld op Vlan-ID of naam van de radiusserver naar de switches waaraan een eindpunt kan worden toegewezen aan een specifieke Layer 2/Layer 3 LISP-instantie.
- SGT-waarde: met dit kenmerk wordt een SGT ingesteld die een eindpunt toewijst aan deze SGT. Dit zou worden gebruikt voor groepsgebaseerd beleid met betrekking tot dit eindpunt en wijst een SGT-waarde toe aan alle frames die via de fabric worden verzonden en die door dit eindpunt zijn ontstaan.
- Stemautorisatie: Stemapparaten werken op het spraak-vlan. Dit stelt spraakautorisatie in en het eindpunt zou verkeer mogen verzenden en ontvangen in het spraakvlan dat is geconfigureerd op een poort. Dit om spraak- en dataverkeer in hun respectieve VLAN's te scheiden
- Sessietime-out: verschillende eindpunten hebben hun eigen time-outs voor de sessies. Een time-out kan worden verzonden vanaf de radiusserver om aan te geven hoe vaak een client opnieuw moet worden geverifieerd
- Sjabloon: voor sommige eindpunten moet een andere sjabloon op een poort worden toegepast om correct te werken. Een sjabloonnaam kan worden verzonden vanaf de Radius-server die aangeeft wat moet worden toegepast op de poort

Controleer het resultaat van de verificatie op een poort met de opdracht toegangssessie weergeven

<#root>

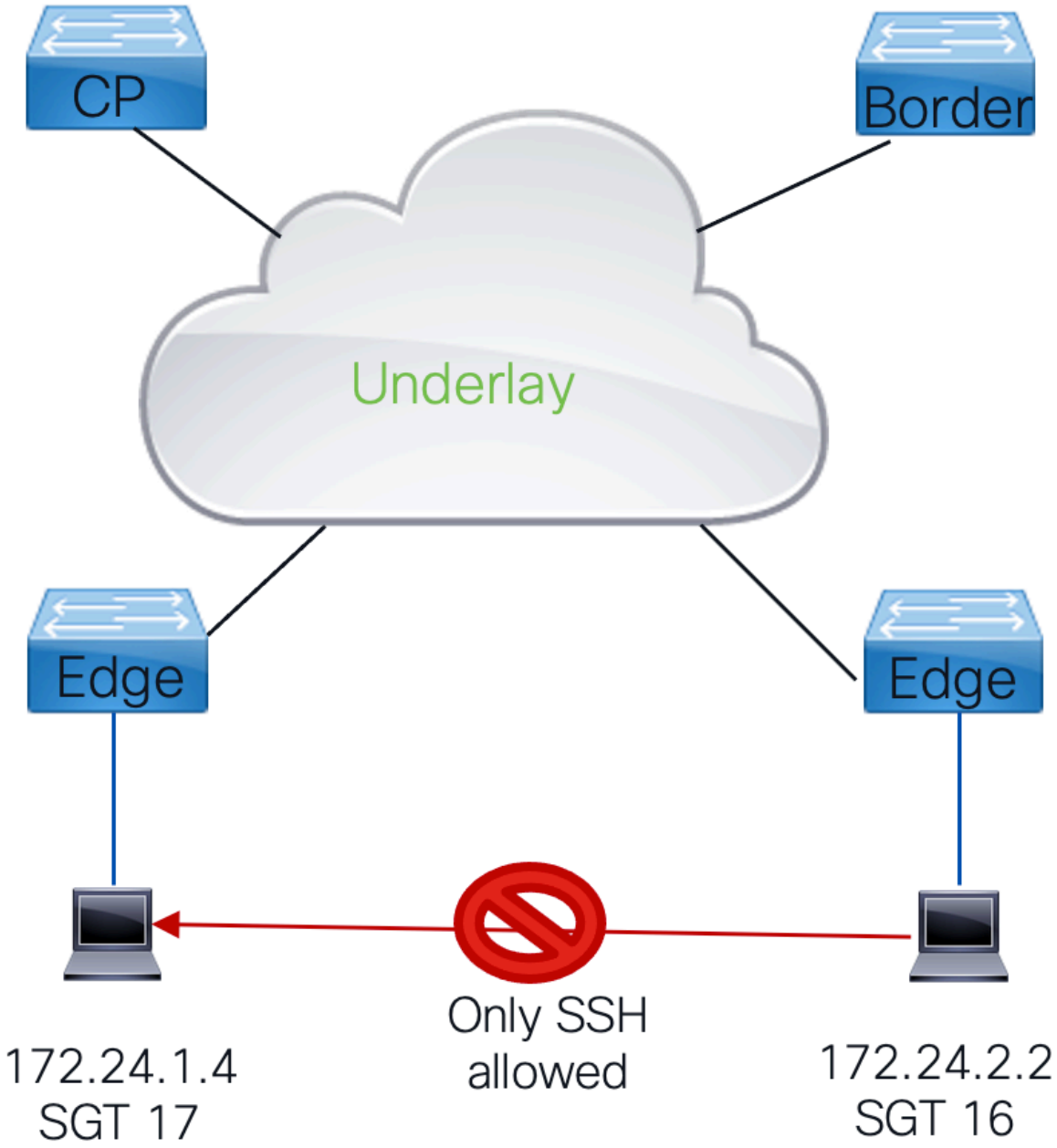
```
FE2067#

show access-session interface Gi1/0/1 details


Interface: GigabitEthernet1/0/1
IIF-ID: 0x1FF97CF7
MAC Address: 0050.5693.f1b2
IPv6 Address: FE80::3EE:5111:BA77:E37D
IPv4 Address: 172.24.1.4
User-Name: 00-50-56-93-F1-B2
Device-type: Microsoft-Workstation
Device-name: W7180-PC
Status:

Authorized


Domain:

DATA


Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Acct update timeout: 172800s (local), Remaining: 172678s
Common Session ID: 9256300A000057B8376D924C
Acct Session ID: 0x00016d77
Handle: 0x85000594
```

```
Current Policy: PMAP_DefaultWiredDot1xClosedAuth_1X_MAB

Local Policies:

Server Policies:

Vlan Group: Vlan: 150


SGT Value: 16


Method status list:
Method State
dot1x

Stopped


mab Authc

Success
```

Let op deze sleutelvelden:

- IPv4- en IPv6-adressen: Meestal geleerd door apparaattracking.
- Gebruikersnaam: Dit is de gebruikersnaam die wordt gebruikt voor verificatie.
    - Voor Dot1x is dit meestal de gebruiker die authenticeert.
    - Wanneer MAB wordt gebruikt, is dit het MAC-adres van het station dat naar Radius wordt verzonden als gebruikersnaam en wachtwoord voor verificatie.
- Status: dit geeft de status van de verificatie en het resultaat van de verificatie aan.
- Domein: Voor normale eindpunten zou dit het Data-domein zijn, dus verkeer zou ongecodeerd op de poort worden verzonden / ontvangen. (Voor spraakapparaten kan dit worden ingesteld op Voice)
- Serverbeleid: Dit is de locatie waar de informatie van de Radius-server, zoals Vlan-toewijzing en SGT-toewijzing
- Methode-statuslijst: Dit toont een overzicht van de methoden die worden uitgevoerd.
    - Standaard dot1x loopt voor MAB.
    - Als een eindpunt niet zou reageren op EAPOL-frames, zou de methode falen tot mab.
    - Dit zou dan laten zien dat dot1x heeft gefaald.
    - MAB toont authentiek succes en geeft aan dat het is gelukt om te authenticeren, het geeft niet aan of het authenticatieresultaat een toegang-accepteren of weigeren zou zijn.

4.2 Verkeersbeleid en groepsbeleid (CTS)



Binnen een LISP VXLAN-fabric wordt CTS gebruikt om verkeersbeleid af te dwingen:

- De op groepen gebaseerde beleidsarchitectuur is gebaseerd op Secure Group-tags.
- Al het verkeer binnen de stof wordt toegewezen op ingress en SGT tag die wordt uitgevoerd door de stof in elk frame.
- Wanneer dit verkeer het weefsel zou verlaten, wordt het verkeersbeleid afgedwongen.
- Dit gebeurt in Groepsgebaseerd beleid dat de bron- en bestemmingsgroeptags van het pakket controleert aan de hand van de matrix die bestaat uit SGT's voor bronbestemming, waarbij het resultaat een SGACL is die definieert welk verkeer wel of niet zou worden toegestaan.
- Wanneer er geen specifieke overeenkomst is binnen de matrix voor de SGT Bron-Bestemming, moet de standaardactie die is gedefinieerd, worden toegepast.

4.3 CTS-omgeving

Om te werken met een groepsbeleid is het eerste dat nodig is voor een Fabric-apparaat om een CTS-pac te krijgen.

- Deze pac moet worden gebruikt in radiusframes om de RADIUS-frames op Cisco ISE te autoriseren. Dit wordt gebruikt om het ct-pac-opaque veld binnen de Radius frames in te stellen.

De CTS-pac-informatie weergeven

<#root>

FE2067#

sh cts pacs

AID:

C7105D0DA108B6AE0FB00499233B9C6A

PAC-Info:
PAC-type = Cisco Trustsec
AID: C7105D0DA108B6AE0FB00499233B9C6A
I-ID: FOC2410L1ZZ
A-ID-Info: Identity Services Engine
Credential Lifetime:

18:05:51 UTC Sat Jun 24 2023

PAC-Opaque: 000200B80003000100040010C7105D0DA108B6AE0FB00499233B9C6A0006009C00030100C5C0B998FB5E8C106F6

Refresh timer is set for 12w0d

Het is belangrijk om ervoor te zorgen dat het CTS-pakket is geconfigureerd en geldig is. Dit wordt automatisch vernieuwd door het Fabric-apparaat.

Opmerking: Als u handmatig een verversing wilt activeren, kan de opdracht "cts ververversen pac" worden uitgegeven.

Voor groepsgebaseerd beleid om te werken, downloadt het omgevingsgegevens en downloadt het de vereiste beleidsinformatie.

- Deze omgevingsgegevens bevatten zowel de CTS-tag die de switch zelf gebruikt als de tabel met alle op groepen gebaseerde beleidsgroepen die op de Radius-server bekend zijn.

CTS-omgevingsgegevens weergeven

<#root>

FE2067#

sh cts environment-data

CTS Environment Data
====================
Current state =

COMPLETE

Last status =

Successful

Service Info Table:
Local Device SGT:
SGT tag =

2-00:TrustSec_Devices

Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
*Server:

10.48.13.221

, port 1812,

A-ID C7105D0DA108B6AE0FB00499233B9C6A

Status = ALIVE
auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Security Group Name Table:
0-00:Unknown
2-00:TrustSec_Devices
3-00:Network_Services
4-00:Employees
5-00:Contractors
6-00:Guests
7-00:Production_Users
8-00:Developers
9-00:Auditors
10-00:Point_of_Sale_Systems
11-00:Production_Servers
12-00:Development_Servers
13-00:Test_Servers
14-00:PCI_Servers
15-00:BYOD
16-00:Fabric_Client_1
17-00:Fabric_Client_2
255-00:Quarantined_Systems
Environment Data Lifetime = 86400 secs
Last update time = 11:46:41 UTC Fri Mar 31 2023
Env-data expires in 0:19:17:04 (dd:hr:mm:sec)
Env-data refreshes in 0:19:17:04 (dd:hr:mm:sec)
Cache data applied = NONE
State Machine is running
Retry_timer (60 secs) is not running

Wanneer op groepen gebaseerd beleid wordt gebruikt, zijn de enige beleidsregels die worden gedownload de CTS-tags waarmee het apparaat lokale eindpunten heeft die het moet afdwingen.

- Om de toewijzing van het IP-adres (of subnet) aan een op een groep gebaseerde beleidsgroep te kunnen controleren, kan de opdracht "show cts role-based sgt-map vrf <vrf> all" worden gebruikt.

Alle bekende IP-naar-SGT-informatie voor een VRF weergeven

<#root>

```
FE2067#
```

sh cts role-based sgt-map vrf Fabric_VN_1 all

```
Active IPv4-SGT Bindings Information
IP Address SGT Source
========================================
```

172.24.1.4 17 LOCAL

172.24.1.254 2 INTERNAL

172.24.2.254 2 INTERNAL

```
IP-SGT Active Bindings Summary
========================================
Total number of LOCAL bindings = 1
Total number of INTERNAL bindings = 2
Total number of active bindings = 3
Active IPv6-SGT Bindings Information
IP Address SGT Source
============================================================
```

2001:DB8::1 2 INTERNAL

2001:DB8::F304:BCCD:6BF3:BFAF 17 LOCAL

```
IP-SGT Active Bindings Summary
========================================
Total number of LOCAL bindings = 1
Total number of INTERNAL bindings = 1
Total number of active bindings = 2
```

Deze uitvoer toont alle bekende IP-adressen (en subnetten) voor een bepaalde VRF en hun groepsgebaseerde beleidsassociaties.

- Zoals te zien is, is er één IP-adres van een eindpunt dat is toegewezen groep gebaseerd beleid groep 17 en dat is lokaal afkomstig.
- Dit is het resultaat van verificatie die plaatsvindt op de poort en waarbij de resultaten aangaven dat de tag is gekoppeld aan dat eindpunt.
- Het benadrukt ook de eigen IP-adressen van de switches, die de device-sgt-tag toegewezen krijgen als interne bron.
- Groepsgebaseerde beleidstags kunnen ook worden toegewezen via configuratie of via een SXP-sessie naar ISE.

Wanneer een apparaat een SGT-tag leert, probeert het de bijbehorende beleidsregels van de ISE-server te downloaden.

- De opdracht toont ct autorisatie vermeldingen geeft een overzicht wanneer die werden geprobeerd te worden gedownload en of ze werden of niet achtereenvolgens gedownload.

Opmerking: Beleid moet periodiek worden vernieuwd in geval van wijzigingen in het beleid. ISE kan ook een CoA-commando pushen voor de switch om te worden geactiveerd om nieuw beleid te downloaden wanneer wijzigingen worden aangebracht. Als u het beleid handmatig wilt vernieuwen, wordt de opdracht "CTS-beleid vernieuwen" gegeven.

Een overzicht weergeven van de beleidsregels die zijn geprobeerd te downloaden en of ze al dan niet achtereenvolgens zijn gedownload

<#root>

```
FE2067#
show cts authorization entries

Authorization Entries Info
==========================
Peer name = Unknown-0
Peer SGT =
0-00:Unknown

Entry State =
COMPLETE

Entry last refresh = 22:14:46 UTC Thu Mar 30 2023
SGT policy last refresh = 22:14:46 UTC Thu Mar 30 2023
SGT policy refresh time = 86400
Policy expires in 0:05:23:44 (dd:hr:mm:sec)
Policy refreshes in 0:05:23:44 (dd:hr:mm:sec)
Retry_timer = not running
Cache data applied = NONE
```

```
Entry status =
SUCCEEDED

AAA Unique-ID = 11

Peer name = Unknown-17
Peer SGT =
17-01:Fabric_Client_2

Entry State =
COMPLETE

Entry last refresh = 11:47:31 UTC Fri Mar 31 2023
SGT policy last refresh = 11:47:31 UTC Fri Mar 31 2023
SGT policy refresh time = 86400
Policy expires in 0:18:56:29 (dd:hr:mm:sec)
Policy refreshes in 0:18:56:29 (dd:hr:mm:sec)
Retry_timer = not running
Cache data applied = NONE
Entry status =
SUCCEEDED

AAA Unique-ID = 4031
```

Als er beleidsregels zijn gedownload, kunnen deze worden weergegeven met het commando "show cts rollebased policies".

```
<#root>

FE2067#
sh cts role-based permissions

IPv4 Role-based permissions
default
:
Permit IP-00

IPv4 Role-based permissions from
group 17:Fabric_Client_2 to group 16:Fabric_Client_1
:
PermitWeb-02

RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

Deze opdracht toont alle beleidsregels die het apparaat heeft geleerd. Op de ISE-server zijn mogelijk meer beleidsregels aanwezig voor verschillende groepen, maar het apparaat probeert alleen beleidsregels te downloaden waarvoor het eindpunten kent. Dit bespaart kostbare hardware.

Deze opdracht toont ook de standaardactie die moet worden toegepast op verkeer waarvoor geen specifiekere vermelding bekend is. In dit geval is het Permit IP, dus al het verkeer dat niet overeenkomt met een specifieke vermelding in de tabel moet worden toegestaan om door te gaan.

Voer show cts rbacl <name>uit om meer details te krijgen over de exacte inhoud van de RBACL die is gedownload

```
<#root>

FE2067#

sh cts rbacl permitssh


CTS RBACL Policy
================
RBACL IP Version Supported: IPv4 & IPv6
name =

permitssh

-03
IP protocol version = IPV4
refcnt = 2
flag = 0x41000000
stale = FALSE
RBACL ACEs:

permit tcp dst eq 22


permit tcp dst eq 23


deny ip
```

In dit geval is het enige verkeer dat naar het eindpunt mag worden verzonden met deze RBACL erop toegepast, tcp-pakketten richting 22 (SSH) en 23 (Telnet).

Opmerking: RBACL werkt slechts in één richting. Tenzij er een beleid is in het retourverkeer, wordt het afgedwongen met het standaardbeleid. Verkeer dat de verbinding binnendringt, wordt niet afgedwongen, het wordt door de verbinding verzonden met de SGT-tag die bekend is op de ingangsnode. Het wordt alleen afgedwongen wanneer het de stof verlaat en het moet worden afgedwongen op het beleid dat op dat apparaat aanwezig

---

is. Doorgaans zouden deze beleidsregels hetzelfde zijn, maar het is mogelijk om het CTS-domein uit te breiden met bijvoorbeeld een firewall waar andere beleidsregels hadden kunnen worden gedefinieerd, afhankelijk van het geïmplementeerde beveiligingsbeleid.

Voer 'op rollen gebaseerde CTS-tellers weergeven' uit om te valideren of frames wel of niet zijn weggelaten

- Deze opdracht toont de gecumuleerde tellers voor de gehele switch. Er is geen equivalente opdracht voor per interface.

<#root>

FE2067#

sh cts role-based counters

Role-based IPv4 counters
From To SW-Denied HW-Denied SW-Permitt HW-Permitt SW-Monitor HW-Monitor

*** ***

0 0 3565235 7777106

0 0

17 16

0

3 0 3412 0

0

16 17

0 5812 0 871231 0

0

Dit overzicht toont alle bekende vermeldingen die de switch in dit geval kent om verkeer van 17 tot 16 en van 16 tot 17 te kunnen matchen.

- Elke andere match die onder de ** valt en de standaardactie krijgt, dus als er verkeer van bijvoorbeeld 18 tot 16 zou komen, komt het niet overeen met de bekende matrix op de switch en wordt de standaardactie toegepast.

Hoewel de tellers cumulatief zijn, geven ze wel een goede indicatie of het verkeer is weggevallen.

- Om te bepalen welk verkeer een item zou raken, kan het logboektrefwoord op de ISE-server worden toegevoegd aan het respectievelijke beleid, wat resulteert in de switch om logboekberichten te verstrekken wanneer dit item wordt geraakt.
- Dit kan gedaan worden voor zowel de standaard actie (**) als een van de meer specifieke items in de matrix.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.